ATTORNEY CONFIDENTIAL

Intel Corporation
4040 Lafayette Center Drive
Chantilly, VA 20151-1218

Intel Legal Team

Fax

Page 1 of 32

Urgent

Confidential

Date: 18-Oct-06

To:	**Fax:**	**Art Unit:**
Examiner: Arezoo Sherkat USPTO	(571) 273-8300	2131
From:	**Fax:**	**M/S:**
Thomas R. Lane Intel Corporation	(703) 633-0933	CY-LF2

Subject: Application No.: 10/082,600

Filed:	**Inventors:**	**Docket No.:**
February 22, 2002	**Grawrock**	**42390P13484**

A CONFIRMATION COPY OF THIS DOCUMENT:

WILL NOT BE SENT

I hereby certify that the below listed correspondence is being facsimile transmitted to the USPTO to: Commissioner for Patents, PO Box 1450, Alexandria, VA 22313-1450 on 10/18/06.
Thomas R. Lane **Date: 10/18/06** _____

Included in this transmission:
Fax Cover Sheet (1 page)
Amended Appeal Brief (31 pages)

RECEIVED
CENTRAL FAX CENTER

OCT 18 2006

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re patent application of:

David W. Grawrock

Serial No.: 10/082,600 Group Art Unit: 2131

Filed: February 22, 2002 Examiner: Arezoo Sherkat

FOR: MULTI-TOKEN SEAL AND UNSEAL

I, Thomas R. Lane, hereby certify that this correspondence is being facsimile transmitted to the United States Patent and Trademark Office on October 18, 2006 and that this paper has been addressed to the Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450, fax number (571) 273-8300.

(Signature of person transmitting correspondence)

AMENDED APPEAL BRIEF

Mail Stop Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

Applicant (hereinafter Appellant) submits this amended appeal brief, in response to the notice of non-compliant appeal brief mailed on August 18, 2006.

The required headings and subject matter follow.

(i) Real party in interest.

This case is assigned of record to Intel Corporation, who is the real party in interest.

(ii) Related appeals and interferences.

There are no known related appeals and/or interferences.

(iii) Status of claims.

Claims 1-44 are pending. Claims 27-34 and claims 41-44 are allowed, claims 1-6, 9-21, 35 and 40 are rejected, and claims 7, 8, 22-26 and 36-39 are objected to. The rejections of claims 1-6, 9-21, 35 and 40 are being appealed.

(iv) Status of amendments.

No amendments were filed subsequent to the final rejection.

(v) Summary of claimed subject matter.

Paragraph numbering of the filed application and the published application may differ. Accordingly, the following description references paragraphs of the present application based upon the paragraph numbering of the application as published on August 28, 2003. Further, supplied reference numbers, paragraphs and elements are not meant to limit the scope of the present claims but merely to provide examples of some elements to aid understanding. The actually claim scope may differ from (and is likely broader than) the example elements given.

Claim 1 is directed to a method comprising requesting a first token (e.g. virtual token 160) to unseal a sealed first portion (e.g. sealed encrypted object SEObj) of a multi-token sealed object to obtain a first portion (e.g. encrypted object EObj) of the multi-token sealed object. See

paragraphs [0053]-[0055] and [0041]-[0047], and step 720 of FIG. 7. The method further comprises requesting a second token (e.g. physical token 150) to unseal a sealed second portion (e.g. sealed key SealK) of a multi-token sealed object to obtain a second portion (key K) of the multi-token sealed object. See, paragraphs [0056] and [0041][0047] and step 730 of FIG. 7. The method also includes using the first portion (e.g. encrypted object EObj) and the second portion (key K) to obtain an object (e.g. object Obj) from the multi-token sealed object. See, paragraph [0057] and step 740 of FIG. 7.

Claim 10 is directed to a method comprising requesting a plurality of tokens (e.g. virtual token 160 and physical token 150) to unseal a plurality sealed portions (e.g. sealed encrypted object SEObj and sealed key SealK) of a multi-token sealed object. See paragraphs [0053]-[0056] and [0041]-[0047], and steps 720 and 730 of FIG. 7. The method further comprises receiving a plurality of unsealed portions (e.g. encrypted object EObj and key K) of the multi-token sealed object. See paragraphs [0053]-[0056] and [0041]-[0047], and steps 720 and 730 of FIG. 7. The method also includes obtaining an object (e.g. object Obj) that has been sealed to the plurality of tokens (e.g. virtual token 160 and physical token 150) using the plurality of unsealed portions (e.g. encrypted object EObj and key K) of the multi-token sealed object. See, paragraph [0057] and step 740 of FIG. 7.

Claim 15 is directed to a method comprising requesting a first token (e.g. virtual token 160) of a computing device (e.g. computing device 100) to seal a first portion (e.g. encrypted object EObj) of a multi-token sealed object to first environment criteria (e.g. environment criteria identified by one or more PCR registers 280 of the virtual token 160). See paragraphs [0048]-[0050] and [0038]-[0040], and step 630 of FIG. 6. The method further comprises requesting a

second token (e.g. physical token 150) of a computing device to seal a second portion (e.g. key K) of the multi-token sealed object to second environment criteria (e.g. environmental criteria identified by one or more PCR registers 240 of the physical token 150). See paragraphs [0051] and [0038]-[0040], and step 640 of FIG. 6.

Claim 35 is directed to a machine readable medium comprising a plurality of instructions that, in response to being executed, result in a computing device sealing a first portion (e.g. encrypted object EObj) of a multi-token sealed object to first environment criteria (e.g. environmental criteria identified by one or more PCR registers of the virtual token 160) using a first public key (e.g. public key 262 or 272) of a first token (e.g. virtual token 160) to obtain a sealed first portion (e.g. sealed encrypted objected SEObj). See paragraphs [0048]-[0050] and [0038]-[0040], and step 630 of FIG. 6. The plurality of instructions further result in the computing device sealing a second portion (e.g. a key K) of the multi-token sealed object to second environment criteria (e.g. environmental criteria identified by one or more PCR registers of the physical token 150) using a second public key (e.g. public key 222 or 232) of a second token (e.g. physical token 150) to obtain a sealed second portion (e.g. sealed key K). See paragraphs [0051] and [0038]-[0040], and step 640 of FIG. 6.

(vi) Grounds of rejection to be reviewed on appeal.

Whether claims 1-6, 9-21, 35 and 40 are anticipated under 35 U.S.C. § 102(e) by Knapton, III (US 6,363,486).

Appellant respectively points out that Knapton appears to qualify as 102(e) prior art and not as 102(b) prior art as proffered by the Final Action. Whether Knapton is 102(b) or 102(e)

prior art should not affect the outcome of the present Appeal. Appellant merely points out the above distinction because Knapton and the present invention were commonly owned at the time of invention, thus disqualifying Knapton from an obviousness rejection under 35 USC 103(c).

(vii) Argument.

Rejection under 35 USC 102(e) over US Patent No. 6,363,486

A claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference. *Verdegaal Bros. v. Union Oil Co. of California*, 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987). Therefore, if even one element or limitation is missing from the cited document, the Official Action has not succeeded in making a prima facie case of anticipation.

Claim 1

Claim 1 requires ***requesting a first token to unseal a sealed first portion*** of a multi-token sealed object to obtain a first portion of the multi-token sealed object, and ***requesting a second token to unseal a sealed second portion*** of a multi-token sealed object to obtain a second portion of the multi-token sealed object. Knapton does not appear to disclose tokens that perform an unseal operation. Accordingly, Knapton does anticipate the invention of claim 1.

In the Official Action dated November 7, 2005, the Official Action appeared to rely on the identifier 230 of the application program 12 and the component identifier 236 of a component (e.g. component 14) for a teaching of a token. However, as indicated in the Response mailed February 7, 2006, the identifiers 230 and 236 appear to be strings of bits which are used as values in the process of generating a component password 240. As such, unlike the tokens of

claim 1, the identifiers appear to be unable to respond to a request let alone unseal portions of an object in response to a request.

To address this apparent deficiency, the Final Action now appears to rely on the application program 12 as the first token and the controller security control 26 as the second token. However, even if the application program 12 and the controller security control 26 could be equated with the first token and second token of claim 1 (a point which the Appellant does not concede), Knapton simply provides no teaching regarding an unseal operation. In support of teaching an unseal operation, the Final Action provides a detailed discussion regarding how Knapton generates a component password 240, and points out that the process of generating the component password 240 includes encryption using well-known DES encryption techniques. The Final Action further states that Knapton ***inherently*** discloses the decryption of the component password when the application program compares the generated component password with the stored component password and allows use of the component if there is a match.

However, Knapton does not inherently disclose the above decryption practice. In fact, Knapton explicitly explains how to allow use of the component without performing decryption steps. In particular, Knapton states that both the controller security control 26 and the application program 12 generate the component password 238 using the process depicted in FIG. 4. See, col. 7 lines 29-37. In particular, as outlined in col. 6, lines 1-15, the application license number 230 is encrypted using the secret encryption key 232 to produce the application key 234. Similarly, component identifier 236 is encrypted with the secret encryption key 232 to produce component key 238. The application key 234 and the component key 238 are then encrypted to

produce the component password 240. Since both the controller security control 26 and the application program 12 use the exact same procedure to generate the component password 240, the component password generated by the application program 12 should match the component password generated by the controller security control 26 only if the application identifiers and the component identifiers used by the application program 12 and controller security control 26 match. Accordingly, Knapton teaches how to protect a component using a technique that requires no decryption or unsealing of the component password 240 and the portions that make up the component password 240.

Since Knapton does not disclose or otherwise teach ***requesting a first token to unseal a sealed first portion***, and ***requesting a second token to unseal a sealed second portion*** as required by claim 1, Knapton does not anticipate the invention of claim 1. Appellant respectfully requests the present rejection of claim 1 be reversed.

Claim 2

Claim 2 depends from claim 1 and is therefore allowable for at least the reasons stated above in regard to claim 1. Claim 2 further requires obtaining the object of the multi-token sealed object by using the first portion as a key to decrypt the second portion. As discussed above, Knapton neither explicitly nor inherently discloses decrypting anything using a key. Knapton merely teaches generating a first component password 240 with a controller security control 26 via encryption and generating a second component password 240 with an application program 12 via encryption and allowing use of the component if there is a match between the two generated component passwords 240. Accordingly, Knapton appears to provide no teaching

regarding using a first portion as a key to decrypt a second portion as required by claim 2. Appellant respectfully requests the present rejection of claim 2 be reversed.

Claim 3

Claim 3 depends from claim 1 and is therefore allowable for at least the reasons stated above in regard to claim 1. Claim 3 further requires receiving a key in response to the first token unsealing the sealed first portion, receiving an encrypted object in response to the second token unsealing the second portion, and obtaining the object of the multi-token sealed object by using the key to decrypt the encrypted object. As mentioned above, Knapton does not appear to teach unsealing. Thus, Knapton does not appear to teach receiving a key and an encrypted object in response to unsealing. Further, as mention above, Knapton does not appear to teach decrypting, and, thus does not appear to teach using the key to decrypt the encrypted object. Since Knapton does not teach each and every limitation, Appellant respectfully requests the present rejection of claim 3 be reversed.

Claims 4 and 5

Each of claims 4 and 5 depends from claim 1 and is therefore allowable for at least the reasons stated above in regard to claim 1. Each of claims 4 and 5 further requires generating a key based upon the first portion and the second portion of the multi-token sealed object, and obtaining the object of the multi-token sealed object by using the generated key to decrypt an encrypted object of the multi-token sealed object. As mentioned above, Knapton appears to provide no teaching regarding unsealing and decrypting. Accordingly, Knapton appears to provide no teaching regarding generating a key from two portions obtained from a sealed object

and obtaining the object from the sealed object by using the generated key to decrypt an encrypted object of the sealed object. Thus, Knapton does not appear to teach each and every limitation of claims 4 and 5. Accordingly, Appellant respectfully requests reversal of the present rejection of claims 4 and 5

Claims 6 and 9

Each of claims 6 and 9 depends from claim 1 and is therefore allowable for at least the reasons stated above in regard to claim 1. Each of claims 6 and 9 further requires receiving a first key and a second key in response to unsealing portions of the multi-token sealed object, generating a third key from the first and second key, and obtaining the object by using the third key to decrypt an encrypted objected. As mentioned above, Knapton does not appear to teach unsealing. Accordingly, Knapton does not appear to teach receiving a first key and a second key in response to unsealing portions of the multi-token sealed object. Also, as mentioned above, Knapton does not appear to teach decryption, and therefore does not appear to teach obtaining the object using a third key to decrypt an encrypted object. Appellant respectfully requests reversal of the present rejection of claims 6 and 9.

Claim 10

Claim 10 requires requesting a plurality of tokens ***to unseal*** a plurality of sealed portions of a multi-token sealed object. As mentioned above, Knapton does not appear to teach unsealing. Accordingly, Knapton does not appear to teach each and every limitation of claim 10. Appellant respectfully requests the rejection of claim 10 be reversed.

Claims 11-14

Each of claims 11-14 depends from claim 10 and is therefore allowable for at least the reasons stated above in regard to claim 10. Each of claims 11-14 also requires generating a key from a plurality of unsealed portions of the multi-token sealed object, and decrypting an encrypted object using the key. As mentioned above, Knapton does not appear to teach unsealing. Accordingly, Knapton does not appear to teach generating a key from a plurality of unsealed portions of the multi-token sealed object. As also mention above, Knapton does not appear to teach decryption. Accordingly, Knapton does not appear to teach decrypting an encrypted object using the key. Since Knapton does not teach each and every limitation of claims 11-14, Appellant respectfully requests the present rejection of claims 11-14 be reversed.

Claims 15-21

Each of claims 15 requires requesting a first token of a computing device to seal a first portion of a multi-token sealed object to a first environment criteria, and requesting a second token of a computer device to seal a second portion of the multi-token sealed object to second environment criteria. As a result, each of claims 15-21 requires requesting two tokens to seal two portions of a multi-token sealed object. Further, each of claims 15-21 requires the first token to seal a first portion to first environment criteria and requires the second token to seal a second portion to second environment criteria.

It is unclear to the Appellant what exactly in Knapton the Final Action is relying on for the first token, the second token, the first portion, the second portion, the first environment criteria, and the second environment criteria despite requesting clarification on at least some of

these aspects in the Response mailed February 7, 2006. Appellant's best guess is that the Final Action equates the application program 12 and the controller security control 26 with the first token and second token of claim 15. Further, the Final Action appears to equate the application key 234 and the component key 238 with the first portion and the second portion of claim 15. As discussed above, the application program 12 and the controller security control 26 each generate a separate component password 240. Accordingly, even if the application program 12 and the controller security control 26 were equated with the first token and the second token (a point the Appellant does not concede), they do not appear to operate on portions of the same object as required by claim 15. In particular, the application program 12 and controller security control 26 do not appear to seal a first portion and a second portion of the same "multi-token sealed object" instead they both appear to generate separate component passwords 240.

Furthermore, Knapton does not appear to disclose requesting a first token to seal to ***first environment criteria*** and requesting a second token to seal to ***second environment criteria***. For such a teaching, the Final Action appears to rely on Knapton disclosing "a component functions only with the component licensed. If another copy of the application program attempts to access the component (e.g., the component was copied to another computer system having an application program with a different license number), the component will not be snapped in." While the above describes the functionality of Knapton, it does not appear to identify what the Final Action regards as "first environment criteria" and "second environment criteria". Also, the above does not appear to identify that a first token seals a first portion of a multi-token sealed object to the first environment criteria and the second token seals the second portion of multi-token sealed object to the second environment criteria.

Since Knapton does not appear to teach each and every limitation of claims 15-21, Appellant respectfully requests the present rejection of claims 15-21 be withdrawn.

Claim 35

Claim 35 requires sealing a first portion of a multi-token sealed object to first environment criteria using ***a first public key*** of a first token to obtain a sealed first portion, and sealing a second portion of the multi-token sealed object to second environment criteria using ***a second public key*** of a second token to obtain a sealed second portion. The reasons presented above in regard to claims 15-21 are relevant to the patentability of claim 35. Furthermore, claim 35 requires using ***public keys*** to seal the first portion and the second portion. Knapton appears to teach the use of ***private keys*** to generate the component password 240. See, Knapton at col. 5, lines 43-45. Accordingly, Knapton does not appear to teach each and every limitation of claim 35. Appellant respectfully requests the reversal of the present rejection of claim 35.

Claim 40

Claim 40 requires unsealing the sealed first portion and unsealing the sealed second portion. As mentioned above in regard to claim 1, Knapton does not appear to provide any teaching regarding "unsealing". Accordingly, Knapton does not anticipate the invention of Appellant's claim 40. Reversal of the rejection of claim 40 is respectfully requested.

CONCLUSION

In view of the foregoing, favorable reconsideration and reversal of the rejections is respectfully requested. Please charge any necessary fees, including extension fees, to our Deposit Account No. 50-0221.

Respectfully submitted,

Date: October 18, 2006

Thomas R. Lane
Reg No. 42,781

(viii) Claims appendix.

1. (Original) A method comprising

requesting a first token to unseal a sealed first portion of a multi-token sealed object to obtain a first portion of the multi-token sealed object,

requesting a second token to unseal a sealed second portion of a multi-token sealed object to obtain a second portion of the multi-token sealed object, and

using the first portion and the second portion to obtain an object from the multi-token sealed object.

2. (Original) The method of claim 1 further comprising obtaining the object of the multi-token sealed object by using the first portion as a key to decrypt the second portion .

3. (Original) The method of claim 1 further comprising

receiving a key in response to the first token unsealing the sealed first portion,

receiving an encrypted object in response to the second token unsealing the second portion, and

obtaining the object of the multi-token sealed object by using the key to decrypt the encrypted object.

4. (Original) The method of claim 1 further comprising

generating a key based upon the first portion and the second portion of the multi-token sealed object, and

obtaining the object of the multi-token sealed object by using the generated key to decrypt an encrypted object of the multi-token sealed object.

5. (Original) The method of claim 1 further comprising

generating a key from the first portion and the second portion of the multi-token sealed object, and

obtaining the object of the multi-token sealed object by using the generated key and an a symmetric cryptographic algorithm to decrypt an encrypted object of the multi-token sealed object.

6. (Original) The method of claim 1 further comprising

receiving a first key in response to the first token unsealing the sealed first portion,

receiving a second key in response to the second token unsealing the second portion,

generating a third key from the first key and the second key, and

obtaining the object of the multi-token sealed by using the third key to decrypt an encrypted object of the multi-token sealed object.

7. (Original) The method of claim 1 further comprising

receiving a first key in response to the first token unsealing the sealed first portion only if the first token determines that a current device environment satisfies environment criteria specified for the sealed first portion,

receiving a second key in response to the second token unsealing the second portion only if the second token determines that the current device environment satisfies environment criteria specified for the sealed second portion,

generating a third key from the first key and the second key, and

obtaining the object of the multi-token sealed by using the third key to decrypt an encrypted object of the multi-token sealed object.

8. (Original) The method of claim 7 further comprising

receiving the first key in response to the first token unsealing the sealed first portion only if a first value computed from the first portion and a first seal record of the sealed first portion has a predetermined relationship with a first digest value of the sealed first portion, and

receiving the second key in response to the second token unsealing the sealed second portion only if a second value computed from the second portion and a second seal record of the sealed second portion has a predetermined relationship with a second digest value of the sealed second portion.

9. (Original) The method of claim 1 further comprising

receiving a first key in response to the first token unsealing the sealed first portion only if the first token generated the sealed first portion,

receiving a second key in response to the second token unsealing the second portion only if the second token generated the sealed second portion,

generating a third key from the first key and the second key, and

obtaining the object of the multi-token sealed by using the third key to decrypt an encrypted object of the multi-token sealed object.

10. (Original) A method comprising

requesting a plurality of tokens to unseal a plurality sealed portions of a multi-token sealed object,

receiving a plurality of unsealed portions of the multi-token sealed object, and

obtaining an object that has been sealed to the plurality of tokens using the plurality of unsealed portions of the multi-token sealed object.

11. (Original) The method of claim 10 wherein obtaining comprises

generating a key from the plurality of unsealed portions of the multi-token sealed object, and

decrypting an encrypted object using the key to obtain the object.

12. (Original) The method of claim 10 wherein obtaining comprises

generating a key from the plurality of unsealed portions of the multi-token sealed object, and

decrypting an encrypted object using the key and a symmetric cryptographic algorithm to obtain the object.

13. (Original) The method of claim 12 further comprising unsealing the plurality of sealed portions only if a current device environment satisfies device criteria specified for the plurality of sealed portions.

14. (Original) The method of claim 12 further comprising unsealing the plurality of sealed portions only if the plurality of tokens generated the plurality of sealed portions.

15. (Original) A method comprising

requesting a first token of a computing device to seal a first portion of a multi-token sealed object to first environment criteria, and

requesting a second token of a computing device to seal a second portion of the multi-token sealed object to second environment criteria.

16. (Original) The method of claim 15 further comprising

encrypting an object using a symmetric cryptographic algorithm and a key to obtain an encrypted object, and

receiving a sealed encrypted object in response to the first token sealing the first portion that comprises the encrypted object,

receiving a sealed key in response to the second token sealing the second portion that comprises the key.

17. (Original) The method of claim 15 further comprising

encrypting the object using an asymmetric cryptographic algorithm and an encryption key of an asymmetric key pair to obtain an encrypted object,

receiving a sealed encrypted object in response to the first token sealing the first portion that comprises the encrypted object,

receiving a sealed decryption key in response to the second token sealing the second portion that comprises a decryption key of the asymmetric key pair.

18. (Original) The method of claim 15 further comprising

receiving a sealed first portion encrypted by the first token using a first key of the first token, the sealed first portion comprising the first key, a first seal record comprising one or more metrics specified by the first environment criteria, and a first digest value that attests to the integrity of the first key and the first seal record, and

receiving a sealed second portion encrypted by the second token using a second key of the second token, the sealed second portion comprising the second key, a second seal record comprising one or more metrics specified by the second environment criteria, and a second digest value that attests to the integrity of the second key and the second seal record.

19. (Original) The method of claim 18 wherein

the first seal record comprises a unique first identifier for the first token, and

the second seal record comprises a unique second identifier for the second token.

20. (Original) The method of claim 15 further comprising

encrypting the object using key that was generated based upon a first key and a second key,

receiving a sealed first key in response to the first token sealing the first portion that comprises the first key,

receiving a sealed second key in response to the second token sealing the second portion that comprises the second key.

21. (Original) The method of claim 20 further comprising

generating a sealed first portion by encrypting the first portion and metrics specified by the first environment criteria using a first key of the first token, and

generating a sealed second portion by encrypting the second portion and metrics specified by the second environment criteria using a second key of the second token.

22. (Original) The method of claim 21 wherein

the first token comprises a virtual token, and

the second token comprises a physical token.

23. (Original) The method of claim 22 further comprising

specifying the second environment criteria by identifying at least one configuration register of the physical token that comprises a metric of the virtual token.

24. (Original) The method of claim 15 further comprising

specifying the first environment criteria by identifying one or more configuration registers of the first token that record metrics of the computing device, and

specifying the second environment criteria by identifying one or more configuration registers of the second token that record metrics of the computing device.

25. (Original) The method of claim 24 wherein

specifying the second environment criteria comprises identifying at least one configuration register of the second token that comprises a metric of the first token.

26. (Original) The method of claim 25 wherein

the first token comprises a virtual token, and

the second token comprises a physical token.

27. (Original) A device comprising

a virtual token comprising one or more configuration registers that record metrics of a device environment and one or more processing units to generate a sealed first key that comprises a first key sealed to first environment criteria,

a physical token comprising one or more configuration registers that record metrics of the device environment, and one or more processing units to generate a sealed second key that comprises a second key sealed to second environment criteria, and

a sealing component to generate a third key based upon the first key and the second key, encrypt an object using the third key to obtain an encrypted object, request the virtual token to seal the first key to obtain the sealed first key, and request the physical token to seal the second key to obtain the sealed second key.

28. (Original) The device of claim 27 wherein the sealing component specifies the first environment criteria by identifying one or more configuration registers of the virtual token to which to seal the first key, and specifies the second environment criteria by identifying one or more configuration registers of the physical token to which to seal the second key.

29. (Original) The device of claim 28 wherein the sealing component specifies a first public key of the virtual token with which to seal the first key, and specifies a second public key of the physical token with which to seal the second key.

30. (Original) The device of claim 29 wherein

the virtual token generates the sealed first key by using the first public key to encrypt the first key, a first seal record comprising metrics specified by the first environment criteria, and a first digest value that attests to the integrity of the first key and the first seal record, and

the physical token generates the sealed second key by using the second public key to encrypt the second key, a second seal record comprising metrics specified by the second environment criteria, and a second digest value that attests to the integrity of the second key and the second seal record.

31. (Original) The device of claim 27 further comprising an unsealing component to request the virtual token to unseal the sealed first key to obtain the first key, to request the physical token to unseal the sealed second key to obtain the second key, to generate a third key based upon the first key and the second key, and to decrypt the encrypted object using the third key.

32. (Original) The device of claim 31 wherein

the processing units of the virtual token further unseal the sealed first key and provide the unsealing component with the first key only if the metrics of the one or more configuration registers of the virtual token satisfy the first environment criteria, and

the processing units of the physical token further unseal the sealed key and provide the unsealing with the key used to decrypt the encrypted object only if the metrics of the one or more configuration registers of the physical token satisfy the second environment criteria.

33. (Original) The device of claim 32 wherein

the virtual token unseals the sealed object by decrypting the sealed object using a first private key of the virtual token to obtain the encrypted object, a first seal record, and a first digest value that attests to the integrity of the encrypted object and the first seal record, and

the physical token unseals the sealed key by decrypting the sealed key using a second private key of the physical token to obtain the key, a second seal record, and a second digest value that attests to the integrity of the key and the second seal record.

34. (Original) The device of claim 31 wherein

the processing units of the virtual token provide the unsealing component with the encrypted object only if the first digest value obtained from the sealed first key has a predetermined relationship with a value computed from the first key and the first seal record of the sealed first key, and

the processing units of the physical token provide the unsealing component with the second key only if the second digest value obtained from the sealed second key has a predetermined relationship with a value computed from the second key and the second seal record of the sealed second key.

35. (Original) A machine readable medium comprising a plurality of instructions that, in response to being executed, result in a computing device

sealing a first portion of a multi-token sealed object to first environment criteria using a first public key of a first token to obtain a sealed first portion, and

sealing a second portion of the multi-token sealed object to second environment criteria using a second public key of a second token to obtain a sealed second portion.

36. (Original) The machine readable medium of claim 35 wherein the plurality of instructions further result in the computing device

specifying the first environment criteria by identifying one or more configuration registers of the first token that record metrics of the computing device, and

specifying the second environment criteria by identifying one or more configuration registers of the second token that record metrics of the computing device.

37. (Original) The machine readable medium of claim 36 wherein the plurality of instructions further result in the computing device

generating the sealed first portion such that the sealed first portion comprises the first portion, a first seal record comprising the metrics of the one or more configuration registers specified by the first environment criteria, and a first digest value of the encrypted object and the seal record, and

generating the sealed second portion such that the sealed second portion comprises the second portion, a second seal record comprising the metrics of the one or more configuration registers specified by the second environment criteria, and a second digest value of the key and the second seal record.

38. (Original) The machine readable medium of claim 37 wherein the plurality of instructions further result in the computing device

unsealing the sealed first portion using a first private key of the first token and providing the first portion only if the metrics recorded by the first token have a predetermined relationship with the metrics of the first seal record, and

unsealing the sealed second portion using a second private key of the second token and providing the second portion only if the metrics recorded by the second token have a predetermined relationship with the metrics of the second seal record.

39. (Original) The machine readable medium of claim 38 wherein the plurality of instructions further result in the computing device

providing the first portion only if the first digest value obtained from the sealed encrypted object has a predetermined relationship to a first value computed from the encrypted object and the first seal record, and

providing the second portion only if the second digest value obtained from the sealed key has a predetermined relationship to a second value computed from the key and the second seal record.

40. (Original) The machine readable medium of claim 35 wherein the plurality of instructions further result in the computing device

unsealing the sealed first portion using a first private key of the first token and providing the first portion object only if a current device environment satisfies the first environment criteria, and

unsealing the sealed second portion using a second private key of the second token and providing the second portion only if the current device environment satisfies the second environment criteria.

41. (Original) A device comprising

a chipset,

a processor coupled to the chipset,

memory coupled to the chipset, the memory comprising a plurality of instructions that, when executed by the processor, result in the processor implementing a virtual token that records metrics of a device environment, that receives a first key used to generate a decryption key, and that seals the first key to one or more metrics recorded by the virtual token in response to receiving a seal operation request, and

a physical token coupled to the chipset, the physical token to record metrics of the device environment, to receive a second key used to generate the decryption key, and to seal the second key to one or more metrics recorded by the physical token in response to receiving a seal operation request.

42. (Original) The device of claim 41 wherein the one or more metrics recorded by the physical token comprises a virtual token metric and the physical token seals the key to at least the virtual token metric.

43. (Original) The device of claim 41 wherein the one or more metrics recorded by the physical token comprises a metric of the plurality of instructions that result in the processor implementing the virtual token and the physical token seals the key to at least the metric of the plurality of instructions.

44. (Original) The device of claim 41 wherein

the plurality of instructions, in response to execution, result in the processor generating a sealed first key that comprises the first key and a unique first identifier for the virtual token, and

the physical token generates a sealed second key that comprises the second key and a unique second identifier for the physical token.

(ix) Evidence appendix.

None.

(x) Related proceedings appendix.

None.